Enhancing your Smartphone Security, Privacy and Anonymity

Michel NALLINO

Nice, France, 2026-09-23 - Revision 22

Copyright Michel NALLINO 2025–2026.

This work is distributed under Creative Commons license, Attribution-NonCommercial 4.0 International (CC BY-NC 4.0), see https://creativecommons.org/licenses/by-nc/4.0/

Disclaimer:

THERE IS NO WARRANTY FOR THE DOCUMENT CONTENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW.

THE COPYRIGHT HOLDER PROVIDES THE DOCUMENT CONTENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

THE ENTIRE RISK AS TO USE OF THE DOCUMENT CONTENT IS WITH YOU. SHOULD THE DOCUMENT CONTENT PROVE WRONG, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Document Internal Links

1. Introduction
2. Filtering DNS resolvers
    - 2.1) Cloudflare with malware block
    - 2.2) Cloudflare with malware and adult content block
    - 2.3) OpenDNS Family Shield
    - 2.4) Rethink configurable DNS resolver
    - 2.5) uBlockDNS configurable DNS resolver
    - 2.6) Recursive DNS Resolvers, sovereign and GDPR-compliant, for EU citizens
3. Android devices
    - 3.1) Introduction to Android
    - 3.2) Use of alternative distributions
        - Linux distributions
            - Ubuntu Touch
            - Sailfish OS
            - PostmarketOS
            - Mobian
            - Plasma Mobile
            - PureOS
        - Android alternative distributions
            - /e/OS
            - LineageOS
            - iodéOS
            - GrapheneOS
            - Huawei
            - XDA Developers
    - 3.3) Use of commercial Android devices
        - Protection against malware, ads and tracking
        - Partial deGoogling

Choice of browser

A zoom on Firefox and Cromite

Other precautions

VPN

Anonymity

4. iPhones

4.1) Introduction to iPhones

4.2) Protection against malware, ads and tracking in iOS

Other precautions on iOS

VPN on iOS

Anonymity on iOS

1. Introduction

Smartphones have invaded our lives, to the point that they sometimes appear as absolutely necessary.

However, though practical, they are often perceived as "Spies in the pocket", to the point that some people refuse to use them.

The goal of this small guide is to show how to enhance your smartphone security, privacy, and anonymity, whatever the kind of your device, Android smartphone or Apple iPhone.

Some figures: There are today ~ 8.6 billion smartphones used in the world, by ~ 7.3 billion users. Android active smartphones are some ~ 5.4 to 5.6 billions, and active iPhones are more than 1 billion.

2. Filtering DNS resolvers

Filtering DNS resolvers are a common tool to increase Android devices and iPhones security and Privacy.

So, this chapter is valid for both kind of devices, and the way to use them will be explained in the Android devices and iPhones dedicated chapters.

2.1) Cloudflare with malware block:

Primary server IPV4 address: 1.1.1.2

Secondary server IPV4 address: 1.0.0.2

Primary server IPV6 address: 2606:4700:4700::1112

Secondary server IPV6 address: 2606:4700:4700::1002

DNS over HTTPS: https://security.cloudflare-dns.com/dns-query

DNS over TLS: security.cloudflare-dns.com

2.2) Cloudflare with malware and adult content block:

Primary server IPV4 address: 1.1.1.3

Secondary server IPV4 address: 1.0.0.3

Primary server IPV6 address: 2606:4700:4700::1113

Secondary server IPV6 address: 2606:4700:4700::1003

DNS over HTTPS: https://family.cloudflare-dns.com/dns-query

DNS over TLS: family.cloudflare-dns.com

2.3) OpenDNS Family Shield:

Primary server IPV4 address: 208.67.222.123

Secondary server IPV4 address: 208.67.220.123

Primary server IPV6 address: 2620:119:35::123

Secondary server IPV6 address: 2620:119:53::123

DNS over HTTPS: https://doh.familyshield.opendns.com/dns-query

DNS over TLS: familyshield.opendns.com

[NB: Cisco has stopped OpenDNS activities in France, effective on June 28, 2024. See:

https://support.opendns.com/hc/en-us/articles/27951404269204-OpenDNS-Service-Not-Available-To-Users-In-France-and-Portugal (service has been reactivated in Portugal).]

2.4) Rethink configurable DNS resolver:

Rethink offers, for free at the moment, DNS resolver with filters that the user can configure:

- filtering, according to your choice, is done on Rethink servers,

- DNS requests are then sent by Rethink to a network of DNS resolvers (Cloudflare etc.).

There are two ways to configure the filters:

* "advanced" configuration, https://rethinkdns.com/configure, you select the filters you want among more than 190 filters;

* "simple" configuration, from the former web page you click on "simple" button, and you select full categories of filters (Adult, Piracy, Gambling, Dating, Social Media, Security Full, Security Extra, Privacy Lite, Privacy Aggressive, Privacy Extreme);

In both cases, once your selection done, you get a DNS resolver name as DNS over TLS (DoT) or DNS over HTTPS (DoH).

Example: having selected from the simple configuration page "Security Full" and "Privacy Agressive", you get the following DNS resolver DoT name:

"1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com".

You can also use the application "Rethink: DNS + Pare-feu + VPN" and use it to configure the filters.

[NB: at 21st May 2026, Rethink does not offer the possibility of a websites whitelist.]

2.5) uBlockDNS configurable DNS resolver:

This resolver works similarly to Rethink, the filtering and the DNS queries are made on different servers:

- filtering, as per your choice, is done on ublockdns.com servers,

- DNS queries, as per your choice, are done on AdGuard DNS, Cloudfare, Google Public DNS or Quad9.

You go to https://ublockdns.com/, you click on "Get Started" and you get a key (4 small English words) that you save. No email address and no username required. Then you select your profile

(Standard, Family, Strict), eventually select extra filtering lists, and your DNS profile (Automatic, Privacy Focus, Security Focus, Performance Focus and Filtering Focus).

You get a DoT DNS server: "xxxxxxxx.dot.ublockdns.com",

and a DoH one: "https://my.ublockdns.com/xxxxxxxx".

The name "xxxxxxxx" is unique, and attached to the four words key.

2.6) Recursive DNS Resolvers, sovereign and GDPR-compliant, for EU citizens:

Here are sovereign, GDPR-compliant, recursive DNS Resolvers:

- "sovereign": servers are inside EU, and there is at least one server in each of the 27 EU countries,

- "GDPR-compliant": offering the best privacy protection to its users, in accordance with EU General Data Protection Regulation, see https://gdpr-info.eu/,

- "DNSSEC compatible": DNS answers are signed by the servers.

EU founded DNS4EU, see https://www.joindns4.eu/. This DNS exists in five flavors:

Hostname	Ads	Trackers	Malware	Adult
unfiltered.joindns4.eu				
protective.joindns4.eu			✅	
noads.joindns4.eu	✅	✅	✅	
child.joindns4.eu			✅	✅
child-noads.joindns4.eu	✅	✅	✅	✅

Non filtering DNS:

Primary IPV4 DNS server: 86.54.11.100

Secondary IPV4 DNS server: 86.54.11.200

Primary IPV6 DNS server: 2a13:1001::86:54:11:100

Secondary IPV6 DNS server: 2a13:1001::86:54:11:200

DNS over HTTPS: https://unfiltered.joindns4.eu/dns-query

DNS over TLS: unfiltered.joindns4.eu

Protective resolution DNS:

This DNS is a hardened one, security oriented.

Primary IPV4 DNS server: 86.54.11.1

Secondary IPV4 DNS server: 86.54.11.201

Primary IPV6 DNS server: 2a13:1001::86:54:11:1

Secondary IPV6 DNS server: 2a13:1001::86:54:11:201

DNS over HTTPS: https://protective.joindns4.eu/dns-query

DNS over TLS: protective.joindns4.eu

Protective resolution with ad-blocking:

Primary IPV4 DNS server: 86.54.11.13

Secondary IPV4 DNS server: 86.54.11.213

Primary IPV6 DNS server: 2a13:1001::86:54:11:13

Secondary IPV6 DNS server: 2a13:1001::86:54:11:213

DNS over HTTPS: https://noads.joindns4.eu/dns-query

DNS over TLS: noads.joindns4.eu

Protective resolution with child protection:

Primary IPV4 DNS server: 86.54.11.12

Secondary IPV4 DNS server: 86.54.11.212

Primary IPV6 DNS server: 2a13:1001::86:54:11:12

Secondary IPV6 DNS server: 2a13:1001::86:54:11:212

DNS over HTTPS: https://child.joindns4.eu/dns-query

DNS over TLS: child.joindns4.eu

Protective resolution with child protection & ad-blocking:

Primary IPV4 DNS server: 86.54.11.11

Secondary IPV4 DNS server: 86.54.11.211

Primary IPV6 DNS server: 2a13:1001::86:54:11:11

Secondary IPV6 DNS server: 2a13:1001::86:54:11:211

DNS over HTTPS: https:/child-noads.joindns4.eu/dns-query/

DNS over TLS: child-noads.joindns4.eu

3. Android devices

3.1) Introduction to Android

Android devices include an operating system with several layers:

- A Linux kernel, personalized for Android.

- A layer of Open Source Android, AOSP, see https://source.android.com/.

- In most cases, a Google layer (with Google Play, Google Play Service, Google Assistant or Gemini, Android Auto, Google Chrome, Gmail, Google Maps etc.).

- Manufacturer specific drivers and settings.

- In some cases an extra manufacturer layer (example, Samsung) over Google one or partially replacing some Google applications.

- Applications from Google Play Store, or from alternative stores such as Accrescent, Aurora, F-Droid, Obtainium, or installed from an apk file.

*[**NB**: Google intents to restrict the possibility to install applications as apks or coming from another store than its own, see https://keepandroidopen.org/].*

Android security is based on the use of a strong sandbox SELinux (Security Enhanced Linux) + seccompbpf, at the kernel level, that provides full isolation of applications. Each application runs with its unique user identification, applications have no access to system or other applications directories. Authorizations are needed (notifications, access to sensors, sending of background data, use of battery etc.); they are set by default, but user can change them. Some mechanisms allow sharing data and files between sandboxed applications.

All the incoming connections are blocked (an extra firewall would be useful only to block outgoing connections, installing a server on an Android device would require to root it).

Security weaknesses come mainly from the use of malware.

Malware are controlled by Google in its Play Store, and by Google Play Protect on the device; risk to download and install malware is greater when using alternative store or when installing from an apk file.

It is recommended to shut down and restart periodically Android devices, to remove memory persisting malware.

As with any operating system, it is recommended to update it as frequently as possible (system and applications), for bugs and security fixes.

The main problem with Android is tracking: you are tracked by Google and by all the "free" (non-pay) applications installed on the device (and even by some pay ones).

Another problem is ads, being displayed so aggressively inside applications that they prevent their normal use.

3.2) Use of alternative distributions

Some users may install alternative distributions instead the one delivered with their Android smartphone, in order to be completely freed from Google.

It requires user skillfulness, and it is not available for all the devices.

Installing an alternative distribution is risky: it might induce smartphone bricking. This risk is canceled when user buys a smartphone with one of these distributions being installed.

These alternative distributions concern a limited number of devices, for which the drivers sources are available.

Finally, without a Google account, Google cloud backup is not possible; user should set up another backing solution. Some users choose root rsync backup but, some applications such as Netflix will not work once the smartphone is rooted.

→ For all those reasons, it is a niche use.

Here are some alternative distributions:

Linux distributions:

* Ubuntu Touch

https://www.ubuntu-touch.io/

"A whole mobile operating system experience, that is yours".

Ubuntu Touch is a Linux operating system, dedicated to smartphones, totally replacing Android.

It is compatible with the following list of devices: https://devices.ubuntu-touch.io/. It is possible to get it preinstalled on some devices (Volla, Pine64 and FXP).

It uses its own applications. Some Android applications can be run on Ubuntu Touch using applications that allow to run containerized Android applications on Linux systems without the need for a complete Android operating system. There are some 200,000 to 300,000 Ubuntu Touch users.

* Sailfish OS

https://sailfishos.org/

"Sailfish OS is a Linux-based European alternative to dominating mobile operating systems, and the only mobile OS offering an exclusive licensing model for local implementations".

It is compatible with the following devices: https://docs.sailfishos.org/Support/Supported_Devices/.

It uses its own applications store, Jolla Store. There are some 80,000 to 120,000 users, mainly developers.

* PostmarketOS

https://postmarketos.org/

"PostmarketOS develops free and open-source software to extend the life of consumer electronics. By empowering people to have full control of their devices, we promote a healthier and more sustainable society".

It is compatible with the following devices: https://wiki.postmarketos.org/wiki/Devices. There are some 1,000 users.

* Mobian

https://mobian-project.org/

"A Debian derivative for mobile devices".

It is compatible with the following devices: https://wiki.debian.org/Mobian/Devices, mainly Pine64 and OnePlus smartphones. There are some 2,000 to 5,000 users.

* Plasma Mobile

https://plasma-mobile.org

"An ecosystem for telephones that respect privacy, free and secure software".

Plasma mobile can be installed on Linux distributions such as PostmarketOS or Mobian. There are few users of Plasma Mobile, some 1,000, since it is a beginning project.

* PureOS

https://www.pureos.net/

"A fully-convergent, user-friendly, secure and freedom respecting OS for your daily usage. With PureOS, you are the only one in control of your digital life".

PureOS is officially compatible only with Librem 5 smartphone made by Purism.

There are some community projects to have it compatible with PinePhone and some Mobian on Nokia. Purism has delivered some 20,000 Librem 5 with PureOS.

→ Globally, the alternative Linux distributions users on smartphones are some 300,000 to 450,000.

Android alternative distributions:

These distributions can use applications from their own applications store, from alternative stores, or can use Google Play applications through Aurora, or through a sandboxed version of Google Play store (for GrapheneOS only).

* /e/OS

https://e.foundation/e-os/

"/e/OS is a complete, fully "deGoogled", mobile ecosystem"

/e/OS is an open-source mobile operating system paired with carefully selected applications. They form a privacy-enabled internal system for your smartphone. And it is not just claims: open-source means auditable privacy. /e/OS has received academic recognition from researchers at the University of Edinburgh and Trinity College of Dublin.

/e/OS could have just focused on an OS, but apps and online services are crucial components of everyday experience, too.

These online services, including search engine, email platform, cloud storage and other online tools, create a unique privacy enhanced environment.

It is compatible with the following list of devices: https://doc.e.foundation/devices. Murena sells some smartphones with preinstalled /e/OS.

Applications are installed from App Lounge: the App Lounge is the second iteration of the application store embedded within /e/OS. It allows everyone to access millions of applications directly from their phone home screen.

It combines common Android apps, open source apps and even progressive web apps in one single repository. It is the only app store that does this today. You don't need to sign in to an account to download apps. There are some 200,000 /e/OS users.

* LineageOS

https://lineageos.org/

"A free and open-source operating system for various devices, based on the Android mobile platform".

It is the successor of CyanogenMod.

It is compatible with the following list of devices: https://wiki.lineageos.org/devices/.

It includes a set of Open Source applications. Google applications are not bundled with LineageOS but can be downloaded separately. There are some 1,800,000 LineageOS users.

* iodéOS

https://iode.tech/

"Google-free Android

iodéOS is an android operating system freed from Google trackers. A significant part of data breaches comes upstream of apps. iodéOS is powered by "LineageOS", an open source OS that expands functionalities and the lifespan of mobile devices of more than 20 different manufacturers thanks to a community of contributors across the world. The Trust interface will help you understand the security of your device and warn incoming threats".

iodéOS is compatible with the following devices:

https://iode.tech/iodeos-official-supported-devices/

Smartphones on which iodéOS is installed are for sale on the site:

https://shop.iode.tech/

* GrapheneOS

https://grapheneos.org/

"The private and secure mobile operating system with Android app compatibility. Developed as a non-profit open source project".

It is compatible with the following list of devices: https://grapheneos.org/faq#supported-devices, only some Google Pixel, because of GrapheneOS security hardware requirements.

GrapheneOS is a security hardened version of Android, Google free, with its own AppStore. Google Play Store can be optionally installed in a sandbox.

GrapheneOS probably provides the best compatibility with Google Play Store applications. There are some 60,000 GrapheneOS users.

* CalyxOS and Pixel Experience are no longer maintained.

→ Globally, taking into account Calyxos and Pixel Experience users, there are some 2,600,000 alternative Android distributions users.

* Huawei

https://consumer.huawei.com

The case of Huawei is specific: Huawei sells Android smartphones, without any access to Google software.

Huawei smartphones do not have access to Google Play Store or to Google applications; they have access to their own app store and to alternate stores (including Aurora for Play Store applications).

In a way, Huawei smartphone users are free from Google tracking, but it has just been replaced by Huawei one!

* XDA Developers

https://xdaforums.com/

On XDA Developers forums, you can find some customized ROMs for some Android devices.

3.3) Use of commercial Android devices

Most Android users use Android devices with the manufacturer provided operating system (Android 14, 15, 16…) and its tailoring.

However, user can set its commercial Android device up in order to enhance its security, privacy, and even have some anonymity.

Protection against malware, ads and tracking

This part does also apply to Android smartphones with alternative Android distribution.

We are speaking here of malware on internet, not of the malware that you can install from stores. The best filtering DNS resolvers, regarding malware protection are:

"protective.joindns4.eu" and other filtering DNS resolvers from the joindns4eu family, it includes a database of more than twenty million malevolent websites; this database is continuously updated, AI is used to analyze the websites behavior.

1st Method: use of a filtering DNS resolver and of DuckDuckGo browser.

Choose the filtering DNS resolver you want, see Filtering DNS resolvers, and enter its DoT name in the private DNS setting found in settings/internet and network.

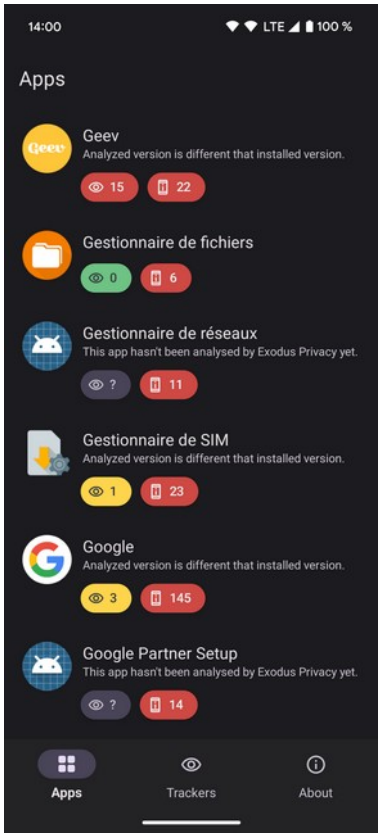
Examples:

> "noads.joindns4.eu" for security enhanced and ads blocking DNS4EU resolver,
>
> "1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com" for a rethink DNS resolver with "Security Full" and "Privacy Agressive" settings,
>
> "xxxxxxxx.dot.ublockdns.com", with the filtering lists and the DNS resolvers of your choice.

The filtering will be system-wide, for all the installed applications and the operating system.

Install DuckDuckGo browser from Play Store. DuckDuckGo browser is a bad browser (no extension, leaking the internal IP address through WebRTC leak, no ads blocking), but we will use it just to add an extra tracking filtering layer over the applications installed on the device, using its App Tracking Protection. More: read https://duckduckgo.com/duckduckgo-help-pages/p-app-tracking-protection/what-is-app-tracking-protection.

App tracking is different from the usual tracking that occurs when using a browser; trackers are specific ones. You can install on your Android smartphone Exodus Privacy application; it will analyze the apps installed on your smartphone and download reports giving, for each app, the trackers used by the app and the list of authorizations requested by the app.



Coupling both filtering DNS resolver and DuckDuckGo App Tracking Protection can protect your Android Device against malware, ads and tracking.

2nd Method: use of personalDNSfilter

personalDNSfilter is an application that can be downloaded from Google Play Store and can be used on a standard non-rooted Android device.

It combines the use of the DNS resolver of your choice, using IPV4 or IPV6 addresses (this excludes Rethink and uBlockDNS DNS resolvers), with a set of filters, accepting two syntaxes: hosts files or DNS filters. You can choose one or several of the preexisting filters, or add a filter of your choice.

More: read https://www.zenz-solutions.de/personaldnsfilter-wp/.

I use "noads.joindns4.eu"as filtering DNS resolver, in DoT mode, with the following IP addresses:

86.54.11.13

86.54.11.213

2a13:1001::86:54:11:13

2a13:1001::86:54:11:213

Here are the filters lists I use (malware, ads, tracking and social networks):

Ads:
https://v.firebog.net/hosts/AdguardDNS.txt;
https://v.firebog.net/hosts/Easylist.txt;
https://raw.githubusercontent.com/lassekongo83/Frellwits-filter-lists/master/Frellwits-Swedish-Hosts-File.txt.
Malware:
https://raw.githubusercontent.com/greatis/Anti-WebMiner/master/hosts;
https://raw.githubusercontent.com/hoshsadiq/adblock-nocoin-list/master/hosts.txt;
https://malware-filter.gitlab.io/malware-filter/urlhaus-filter-hosts.txt;
https://urlhaus.abuse.ch/downloads/hostfile/;
https://raw.githubusercontent.com/FadeMind/hosts.extras/master/add.Spam/hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/rpz/tif.mini.txt;
https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/lists/latestdomains.piHole.txt.
Trackers:
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.amazon.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.apple.txt;
https://v.firebog.net/hosts/Easyprivacy.txt;
https://hostfiles.frogeye.fr/multiparty-trackers-hosts.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.huawei.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.winoffice.txt;
https://raw.githubusercontent.com/mullvad/dns-blocklists/refs/heads/main/files/tracker;
https://raw.githubusercontent.com/notracking/hosts-blocklists/master/hostnames.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.oppo-realme.txt;
https://gitlab.com/quidsup/notrack-blocklists/-/raw/master/trackers.hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.tiktok.extended.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.vivo.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.xiaomi.txt.
Multiple filters kinds: *(Ads, Affiliate, Tracking, Metrics, Telemetry, Phishing, Malware, Scam, Fake, Crytojacking and other "Crap").*
https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts;
https://big.oisd.nl/domainswild2;
https://raw.githubusercontent.com/hagezi/dns-blocklists/main/wildcard/pro-onlydomains.txt.
Social networks: *(the use of this list will prevent the use of Facebook, Instagram, Pinterest, Snapchat, Tiktok, X etc., but will allow the use of WhatsApp).*
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/wildcard/social-onlydomains.txt.

With personalDNSfilter, no need of DuckDuckGo browser; moreover, it includes the possibility to whitelist some websites (included in the filters) that you would want to connect to, and to add manually some websites you would want to filter.

Partial deGoogling

This doesn't apply to Android smartphones with alternative Android distribution.
I have uninstalled or deactivated (when uninstalling is not possible) all the Google Applications that I do not use:

- Android Auto,
- Gemini,
- Gmail (replaced by Thunderbird),
- Google,
- Google Assistant,
- Google Chrome (replaced by Firefox),
- Google Docs (replaced by Collabora Office),
- Google Fit,
- Google Maps (can be accessed more privately with a browser),
- Google Meet (can be accessed more privately with a browser),
- Google News (can be accessed more privately with a browser),
- Google TV,
- Google Voice Recognition and Synthesis (keep it and remove microphone authorization if you need to use voice synthesis),
- Notes Keep,
- YouTube (can be accessed more privately with a browser),
- YouTube Music (replaced by VLC).

Choice of browser:

There are two main families of browser available for Android. They can be installed from F-Droid, FFUpdater (in F-Droid store) or from Google Play Store for some:
- Firefox and Firefox based browsers:
Stable versions:

- Firefox, privacy-oriented, lots of extensions available,
- Fennec F-Droid, same as Firefox, without telemetry,
- Firefox Focus, reduced functionalities,
- Firefox Klar, same as Firefox Focus, without telemetry,
- Tor Browser, anonymous browsing using Tor network.

Experimental versions, less tested, less stable:

- Firefox Beta, to test the upcoming version of Firefox,
- Firefox Nightly, for developers, to test future functionalities,
- IronFox, it borrows some functionalities to Firefox Nightly and uses code of former Mull Browser, privacy enhanced,
- Iceraven, providing more options and more possibilities to customize.

- Chromium and Chromium based browsers:

The Chromium family of browsers is reputed to be more secure than Firefox family ones. However, they generally suffer from less privacy.
Stable versions:

- Google Chrome is the worst browser in terms of privacy, tied to Google servers, no extensions,
- Chromium is still tied to Google servers, but less than Chrome,
- Brave Browser, supposed to protect users' privacy, but comes with its own ads,
- Vivaldi Browser, privacy-oriented and ads blocker, but not fully Open Source,
- F-Droid Privacy Browser, privacy-oriented, limited ads blocker,
- Duck Duck Go Browser, privacy-oriented but WebRTC leak, anti-tracking, no ads blocker, no extensions.

Experimental version, less tested, less stable:

- Cromite, security and privacy enhanced, using code of former bromite, integrated ads blocker and anti-fingerprinting, no cast, no DRM videos playing, no extension.

The most reputed browser in terms of security is Vanadium, but it is available only within GrapheneOS since it uses some security features of its distribution.

A zoom on Firefox and Cromite:
Firefox for Android is my default browser, it replaces Google Chrome. It is available from Google Play Store.
Settings:

- "about:config" is available but hidden; it can be accessed with "chrome://geckoview/content/config.xhtml"; make a shortcut.

Make the following changes in "about:config", or check they are already made:

- "browser.cache.disk.enable" set to "false", to disable disk caching,
- "webgl.enable-debug-renderer-info" set to "false", to prevent graphic driver to be exposed,
- "media.peerconnection.enabled" set to "false", to disable WebRTC leak,
- "javascript.options.baselinejit" set to "false", to disable javascript just in time compilation, it reduces javascript attack surface,
- "pdfjs.enableScripting" set to "false", to disable scripting in PDF,
- "network.IDN_show_punycode" set to "true", to be protected against IDN homograph attacks, URLs with non-Latin characters will be displayed as punycode,
- "network.captive-portal-service.enabled" set to "false", to remove Firefox telemetry,
- "captivedetect.canonicalURL", replace the http address by a void chain, to remove Firefox telemetry,
- "dom.fs.enabled" set to "false", to prevent OPFS writing on SSD and avoid OPFS fingerprinting.

I have installed the following extensions:

- "Canvas Blocker", fingerprinting protection,
- "CSS Exfil Protection", privacy protection,
- "Dark Reader", it allows displaying web pages with white characters on black pages, just a question of taste,

- "DuckDuckGo Search and Tracker Protection", privacy protection, it installs DuckDuckGo search as home page, DuckDuckGo search engine by default and DuckDuckGo Privacy Essentials extension,
- "Privacy Badger", privacy protection,
- "Font Fingerprint Defender", fingerprinting protection,
- "uBlock Origin", one of the best ads, privacy and malware filter,
- "NoScript Security Suite", which allows activating javascript only on trusted websites.

Note that not all Firefox extensions are available for Android version of Firefox. However, using the debug mode (type five times on Settings/About Firefox) allows installing any extension from a file.

You may want to install another browser than Firefox: Cromite is a fork of Chromium, based on former Bromite, it is a privacy hardened version of Chromium, with its own filter capability based on AdBlock Plus, still offering full Chromium security. See: https://github.com/uazo/cromite.
It is not available from Google Play Store; to install it you should first download and install F-Droid store, from https://f-droid.org/. Then, to install Cromite, add the following repository to F-Droid: https://www.cromite.org/fdroid/repo/?fingerprint=49F37E74DEE483DCA2B991334FB5A0200787430D0B5F9A783DD5F13695E9517B then look for Cromite in F-Droid and install it.
Note that Cromite is maintained by a very small team and could disappear without notice, as bromite did; check that it is updated regularly.

Here is a comparison of Firefox and Cromite, based on security and privacy aspects:

Feature	**Firefox**	**Cromite**
Sandboxing	Basic	Extra sandboxing (in-app seccomp-bpf)
Isolation from other applications	Basic	Improved (1)
Internal processes are isolated	Yes, Fission (2)	Yes
Tracking protection	Strict (3)	Medium (4)
Telemetry	Yes (can be disabled)	None
Extensions	Yes	No (5)
Local network access restriction	Shipped (6)	Shipped (6)

[NB:
(1): Cromite uses android:isolatedProcess="true" feature in its manifest; it is so executed according to a special process. The only communication with it is via Service API.
(2): Fission is enabled in Firefox for Android from version 147.0.
(3): The strict tracking protection is available, Google Safe Browsing is available and extensions such as uBlock Origin, Privacy Badger, DuckDuckGo Privacy Essentials, Canvas Blocker, Font Fingerprint Defender can be installed.

(4): Cromite includes some fingerprinting prevention techniques and an integrated ads blocker derived from AdBlock Plus, Google Safe Browsing is not available.
(5): The lack of extensions in Cromite prevents the use of uBlock Origin, Privacy Badger, DuckDuckGo Search & Tracker Protection, Canvas Blocker, Font Fingerprint Defender, which impacts ads, privacy and tracking; NoScript, which impacts security; CSS Exfil Protection, which impacts privacy.
(6): Without this restriction, public websites can probe a user's local network, perform CSRF attacks against vulnerable local devices, and generally abuse the user's browser as a "confused deputy" that has access inside the user's local network or software on their local machine. Firefox conforms to Local Network Access specification, https://wicg.github.io/local-network-access/, from version 149, while Chromium based browsers conform from version 152.]

It is possible to use Firefox with an extra isolation, functioning in a work profile:

- Install a F-Froid Store, from https://f-droid.org/.
- From F-Droid, install Shelter.
- Launch Shelter; once the work profile created, disable in the work profile the Google applications you do not use.
- During the work profile creation, Shelter has cloned Play Store.
- From Play Store in work profile, install Firefox.

F-Droid on your personal profile will keep Shelter updated. While Play Store in work profile will keep Firefox updated.
Firefox will run in the work profile, isolated from other applications running in the personal profile.

Other precautions

- It is recommended to shut down and restart periodically Android devices, to remove memory persisting malware.
- Enable localization, NFC, Bluetooth, Wi-Fi only when you need it.
- Never connect to a public Wi-Fi spot.
- For each installed application, set its notifications, authorizations, battery use; revoke permissions that are unnecessary or excessive for the app's functionality.
- Use the "System Manager" application to set the "super energy economy mode", it will prevent most applications to work in the background.
- If the setting is available (Android 14 and later), disable 2G.
- When possible, prefer to use the browser than a dedicated app (example: connect to Facebook with Firefox, don't use Facebook app).
- Keep your Android system, Play Protect and applications updated.
- Use a password manager to store locally all passwords, protect its access with a strong password.
- Use only full End-to-End encrypted communications (do not use SMS any longer; use RCS between Android devices; at the date of April 2026, do not use RCS between Android devices and iPhones; use full End-to-End encrypted messaging application between Android devices and iPhones, see "Anonymity" below).
- Enable Android Safe Browsing protection: when you have removed Google Chrome and other Google apps, the list of applications taking benefit of Safe Browsing is small, but

enabling it will prevent malware and phishing for those applications. URLs you request are sent hashed to Google servers, respecting your privacy. Note that Safe Browsing is included in Firefox, with local verification.

- Enable Google Play Protect.
- When buying a new smartphone, opt for the latest hardware version from the manufacturer, newer hardware often incorporates critical security features that older hardware cannot support. Without the most recent version of the hardware, software updates alone will not provide the maximum available security benefits.

VPN

It is possible to use a VPN in Android devices. Once installed, the VPN connection can be set to permanent in Settings/Internet and Network. The use of a VPN is mandatory with some European ISPs that use IP address to track their users for personalized ads via Utiq (Deutsche Telekom, Telefónica, Vodafone, Orange, Bouygues Telecom, SFR, Free…).

Use a VPN without any logging, such as Proton VPN or Mullvad VPN.

Note that the use of a VPN prevents the use of DuckDuckGo Browser and of personalDNSfilter; though they are not VPNs, they use the VPN setting of Android.

However, there is a way to use a VPN and a filtering DNS resolver. Three methods:
With Proton VPN:

- Install the "Proton VPN" application from Google Play Store and launch the application in "guest" mode or connect in "free" mode.
- In Android's network and internet settings, enter a DNS resolver name filter, as an example "xxxxxxxx.dot.ublockdns.com".
- The internet connection will be via ProtonVPN, and DNS requests will be sent via Proton VPN in secure mode to filtering DNS resolver.

With Rethink:

- Install the "Rethink: DNS VPN Firewall" app from Google Play Store.
- Launch the app and configure filters.
- Download a Wireguard profile for your VPN. For example, for Proton VPN, log in to https://account.protonvpn.com/downloads and download a VPN configuration.
- Import your VPN configuration into the Rethink app.

With Wireguard:

- Install the "Wireguard" app from Google Play Store.
- Download a Wireguard profile for your VPN. For example, for Proton VPN, log in to https://account.protonvpn.com/downloads and download a VPN configuration.
- Launch the app and import the configuration.
- Change the DNS resolvers IP addresses by the ones of the filtering DNS resolver you want.

[NB: it is no longer possible to use "OpenVPN for personalDNSfilter" in conjunction with "personalDNSfilter", the VPN app is old and obsolete.]

Anonymity

Tor Browser is available in the Play Store; use the same settings as for Firefox and do use the built-in NoScript Security Suite extension. However, Tor Browser for Android is currently (April 8, 2026) based on Firefox 140.9 esr, and Fission will be enabled only when Tor Browser will be based on Firefox 147.0 or later. To check if Fission is available:

- "about:config" is available but hidden, like with Firefox; it can be accessed with "chrome://geckoview/content/config.xhtml"; make a shortcut.
- Check that "fission.autostart" and "fission.autostart.session" value is "true".

You may add the same extensions as for Firefox, or a subset (do not add too many extensions to avoid fingerprinting tracking). You can install extensions in Tor Browser using debug mode (tap settings/about Tor Browser five times) which allows you to install any extension from a file.

Here are two methods for more security:
- Use Tor Browser with extra isolation, functioning inside a work profile:

- Install a F-Froid Store, from https://f-droid.org/.
- From F-Droid, install Shelter.
- Launch Shelter; once the work profile created, disable in the work profile the Google applications you do not use.
- During the work profile creation, Shelter has cloned Play Store.
- From Play Store in work profile, install Tor Browser.

F-Droid in your personal profile will keep Shelter updated. Play Store in the work profile will keep Tor Browser updated.
Tor Browser will run in the work profile, isolated from other applications running in the personal profile.
- Use Orbot and launch the browser you want, Firefox or Cromite, with Orbot.
Here is how to launch Firefox with Tor, with Orbot:

- Install Orbot.
- Launch Orbot in advanced user mode.
- In Firefox address bar enter "chrome://geckoview/content/config.xhtml".
- Modify the following values:
  "network.proxy.socks", value "127.0.0.1",
  "network.proxy.socks_port", value "9050",
  "network.proxy.type", value "1".
- Check that Firefox uses Tor: https://check.torproject.org/.

To return to normal, non-Tor mode of Firefox, enter "chrome://geckoview/content/config.xhtml" and change the value of "network.proxy.type" back to "0".

Several messaging applications offer anonymity and full End-to-End Encryption. Avoid WhatsApp (undisclosed source), Telegram (encrypted up to the servers by default, "Secret Chat" option needs to be enabled to have full End-to-End Encryption), prefer Signal or Olvid.

4. iPhones

4.1) Introduction to iPhones

iPhones are exclusively made by Apple; their operating system, iOS, is of the "undisclosed sources" kind, and all the applications are preinstalled by Apple or come from Apple AppStore.

EU has asked Apple to open its smartphones to alternatives stores, threatening Apple with hundreds millions dollars fees; Apple has finally accepted, and removed any difficulty to use an alternative store from iOS 18.6. Of course, the security of apps installed from an alternative store is no longer managed/guaranteed by Apple.

Security is so under the strict control of Apple. Few is known about security weaknesses. Apple "bug bounty" program is recent (2020), the maximum reward is limited to USD 500,000, and some bugs researchers prefer to sell what they find to an Israel company (Pegasus) that pays for that and makes programs able to attack iOS, programs that are sold at very high cost to governments. Overall security seems very good.

Applications are strongly isolated, to the point that they cannot share anything (if you want to use Apple Music and VLC to listen music, you need to copy your music within both the applications directories).

iOS has some protection against tracking, cross applications tracking is just a setting to select, and Safari, the web browser, does include some tracking protection.

Ads seem to be displayed less aggressively in iOS applications than in Android versions of the applications.

4.2) Protection against malware, ads and tracking in iOS

There is only one method that works system-wide: the use of a filtering DNS resolver (see Filtering DNS resolvers).

There is no equivalent of personalDNSfilter for iOS, and DuckDuckGo Browser for iOS cannot work as a tracking protection for applications.

The best filtering DNS resolvers, regarding malware protection are "protective.joindns4.eu" and other filtering DNS resolvers from the joindns4eu family. They include a database of more than twenty million malevolent websites. This database is continuously updated, AI is used to analyze the websites behavior.

If you want to use a filtering DNS resolver with malware and ads filtering, you should use:

- One of the protective DNS4EU resolvers, "noads.joindns4.eu" or "child-noads.joindns4.eu".
- A tailored version of Rethink DNS resolver, example with "Security Full" and "Privacy Aggressive" settings "1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com".
- A tailored version of uBlockDNS, "xxxxxxxx.dot.ublockdns.com".

In order to set DNS resolver in iOS devices, you need a DNS profile; such a DNS profile can be downloaded for DNS4EU and uBlockDNS from their websites (see the links in Filtering DNS resolvers).

Rethink does not offer such a facility. You can generate a DNS profile from Secure DNS profile creator, https://dns.notjakob.com/.

Once you have the profile you need, you import it in your iOS device (send it by mail), install it in General Settings/VPN and device management, and validate it; it will be active in the "Restrictions and Proxies" section.

Browser: there is no need to use any other browser than Safari; because of Apple restrictions, Firefox for iOS is very poor, based on webkit (the same rendering engine as Safari), and has no extension. The only interest is in Firefox Focus, that can be used as a browser with "quick forget" and anti-tracking features; moreover, it can act as a content blocker for Safari.

You can install uBlock Origin Lite extension for Safari; once installed, give it the necessary permissions, set the level of protection and select the lists of filters.

You can complete anti-tracking features using Firefox Focus, and a free version of Adguard or Adblock Plus as extra content blocker (for Safari only). To avoid OPFS fingerprinting, use Safari in private mode (open a new private tab); once the tab is closed, OPFS writings are deleted.

Other precautions on iOS

- It is recommended to shut down and restart periodically iOS devices, to remove memory persisting malware.
- As with any operating system, it is recommended to update it as frequently as possible (iOS system and applications), for bugs and security fixes.
- Enable localization, Bluetooth and Wi-Fi only when you need it.
- Never connect to a public Wi-Fi spot.
- For each installed application, set its notifications, authorizations; revoke permissions that are unnecessary or excessive for the app's functionality.
- Disable Siri, globally and in each application setting.
- Use the energy economy mode permanently, it prevents background applications working.
- Set the cross applications tracking prevention.
- When possible, prefer to use the browser than a dedicated app (example: connect to Facebook with Safari, don't use Facebook app),
- Use a password manager to store locally all passwords, protect its access with a strong password.
- Use only full End-to-End encrypted communications (use iMessages only between iPhones; at the date of April 2026, do not use RCS between iPhones and Android devices; use full End-to-End encrypted messaging application between iPhones and Android devices, see "Anonymity" below).
- Disable the "Send as Text Message" setting to ensure messages do not send as SMS if iMessage is unavailable (iMessage offers end-to-end encryption between Apple users only).
- Enable Lockdown Mode. Lockdown Mode strictly limits certain apps, websites, and features (or makes some features unavailable), reducing the attack surface that could potentially be exploited by threat actors).
- Enroll in Apple iCloud Private Relay. For additional protections, enroll in Apple iCloud Private Relay (see the iCloud User Guide for configuration instructions). Private Relay

ensures iCloud devices use secure DNSs, masks IP addresses, and splits traffic between servers controlled by Apple and a third party to reduce the chances that a single entity can link browser behavior to the user's identity. Note: These benefits are limited to the Safari browser.

- When buying a new iPhone, opt for the latest hardware version, newer hardware often incorporates critical security features that older hardware cannot support. Without the most recent version of the hardware, software updates alone will not provide the maximum available security benefits.

VPN on iOS

The use of a VPN is possible on iOS. See General Settings/VPN and device management. Use a VPN without any logging, such as Proton VPN or Mullvad VPN.

The use of a VPN is mandatory with some European ISPs that use IP address to track their users for personalized ads via Utiq (Deutsche Telekom, Telefónica, Vodafone, Orange, Bouygues Telecom, SFR, Free…).

Anonymity on iOS

Tor Browser is not available from the Play Store, but you can use Onion Browser or Orbot with Safari on iOS (with reduced confidentiality protection because of Apple restrictions, memory is limited to 50 MB and this prevents to find long paths in Tor network).

Several messaging applications offer anonymity and full End-to-End Encryption. Avoid WhatsApp (undisclosed source), Telegram (encrypted up to the servers by default, "Secret Chat" option needs to be enabled to have full End-to-End Encryption), prefer Signal or Olvid.